VOLUME 78 ◆ NUMBER 9

Employee Benefit Plan Review

Business Associate Agreements Matter: Demystifying the Perceived Simplicity of HIPAA Agreements

By Shalyn Watkins

For most healthcare providers and businesses, signing a Business Associate Agreement (BAA) is a standard practice. When contracting to provide services with an entity governed by the Health Insurance Portability and Accountability Act (HIPAA), it is a requirement that the entity enter into a business associate contract, also known as a BAA. This includes HIPAA covered entities, their business associates and downstream business associate subcontractors.

Though it may seem easiest to simply sign a BAA as a standard attachment to a service agreement, this article highlights five of the many reasons why parties should always read, review and negotiate the terms prior to execution.

However, parties often treat the agreements as boilerplate and either fail to read and negotiate their terms or, worse, forego executing the agreement altogether. Contrary to popular belief, though, BAAs are critically important and can make or break a compliance program if not taken seriously.

Though it may seem easiest to simply sign a BAA as a standard attachment to a service agreement, this article highlights five of the many reasons why parties should always read, review and negotiate the terms prior to execution.

What Must a BAA Say?

HIPAA clearly outlines the required elements of a BAA, and the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) provides sample agreements on its website.[1] Though this guidance is helpful, it is important to understand that the sample agreements represent the minimum requirements for BAAs. Pursuant to 45 CFR 164.504(e), a BAA between a covered entity and a business associate must:

- Establish the permitted and required uses and disclosures of protected health information (PHI) by the business associate
- Provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or law

- Require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic PHI
- Require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured PHI
- Require the business associate to disclose PHI as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their PHI, as well as make available PHI for amendments (and incorporate any amendments, if required) and accountings
- To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation
- Require the business associate to make available to HHS its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule
- At termination of the contract, if feasible, require the business associate to return or destroy all PHI received from, or created or received by the business associate on behalf of, the covered entity
- Require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to PHI agree to the same restrictions and conditions that apply to the business associate with respect to such information
- Authorize termination of the contract by the covered entity if the business associate violates a material term of the contract; contracts between business associates and business associates that are subcontractors are subject to these same requirements

These elements must be included in all business associate agreements in order for the agreement to be considered valid.

What Should Parties Consider When Negotiating BAAs?

BAAs should not be viewed as standard boilerplate. They require careful review and consideration by both parties.

1. *Noncompliant and Nonexistent Agreements*. Despite 45 CFR 164.314(a) and 164.502(e) clearly laying out the requirements for BAAs, many parties fail to comply to the basic formalities required under the regulations. Parties without experience working with covered entities often assume that standard confidentiality agreements or nondisclosure agreements will suffice. However, the failure to execute a BAA can result in severe monetary fines arising from multiple HIPAA violations. Disclosure of PHI in the absence of an executed BAA is an impermissible disclosure and potentially a breach requiring notice, as well as a violation of the regulation requiring a BAA.
2. *Old Form Agreements*. Some parties forget to update their BAAs as changes to HIPAA occur. For example, a form agreement that was originally drafted before 2013 would not address the HITECH Act omnibus rule, including the amended definition of a breach, and probably does not address the particular risks related to current operations of the contracting parties. Furthermore, as the OCR continues to promulgate new laws and regulations today, BAAs and HIPAA Policies and Procedures require updating.
3. *Restrictive Agreements*. Since BAAs can include provisions beyond those required under the regulations, it is prudent that business associates read the additional provisions carefully to ensure they are not overly restrictive. The permitted conduct section of the BAA limits the business associate's ability to use or disclose PHI for only the purposes allowed in the agreement. But if that section is missing certain conduct, the business associate may be too restricted and incapable of providing services to the covered entity without violating HIPAA. For example, if a BAA does not include the use and disclosures of PHI for the business associate's own proper management and administration and to fulfill its legal responsibilities in the listing of permitted conduct, it will be difficult, if not impossible, for the business associate to comply with the terms of the agreement. BAAs are not "one-size fits all," and terms should be drafted carefully to ensure sufficient permissions for a business associate to perform its services.
4. *Unclear Reporting Obligations*. Some BAAs attempt to pass the covered entity's obligation to report breaches to the business associate. However, sometimes the business associate is not in the ideal position to effectuate such notices. It is important that business associates accepting this responsibility confirm their reporting obligations and ensure they have the infrastructure to report breaches to individuals, the Secretary of HHS and the media as required by law. Though a covered entity may

delegate reporting obligations to a business associate, the OCR has been clear that the covered entity is ultimately responsible for ensuring that notice is provided in compliance with the breach notification regulations in HIPAA.

5. *Unrealistic Reporting Times*. When security incidents occur, business associates may not immediately be aware. Particularly in situations where the business associate works with independent contractors and parties outside its organization, the business associate is less likely to have immediate knowledge of security incidents and breaches. But if their BAAs require notification within days of the incident's occurrence, the business associate may be in breach of the BAA if it fails to timely report the incident to the covered entity. This creates an impossible situation for business associates, which could be avoided by reading and negotiating the reporting time obligations within the BAA. Though reporting must occur relatively quickly for the covered entity to assess whether a breach has occurred and if notification is required, business associates can request reasonable timing for reporting incidents at the outset.

Though this list is not exhaustive, it represents five of the biggest considerations for parties when entering into BAAs. HIPAA permits the addition of other terms that are not inconsistent with HIPAA. Provisions addressing indemnification, injunctive relief, relationship to state privacy laws and other federal laws – such as Part 2 Privacy and Cures Act information blocking, along with other terms – may be considered. The terms of these agreements can make or break a party's privacy compliance program and should be treated as important topics of negotiation instead of boilerplate.

Note

1. https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

The author, an attorney with Holland & Knight LLP, may be contacted at shalyn.watkins@hklaw.com.